**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF GEORGIA**
**ATLANTA DIVISION**

DONNA CURLING, *et al.*

*Plaintiffs*,

v.

BRAD RAFFENSPERGER, *et al.*,

*Defendants*.

CIVIL ACTION

FILE NO. 1:17-cv-2989-AT

**STATE DEFENDANTS' NOTICE REGARDING SECURITY REVIEW OF DR. HALDERMAN'S MEMORY CARD**

Per this Court's order [Doc. 490], State Defendants identify and explain the proposed protocols regarding the security of Dr. Halderman's memory card. The supporting declarations of Bryan Tyson attached as Ex. A and Theresa Payton attached as Ex. B are sworn statements outlining the proposed security of the review process for the memory card.

**1. Proposed locations for review.**

State Defendants propose two locations for the review of the information on the memory card: (1) the Arlington, VA offices of cybersecurity firm of Fortalice Solutions, under the supervision of Theresa Payton and Paul Brandau; and (2) the offices of Taylor English Duma LLP, under the supervision of counsel. As detailed in the attached declarations, each of these

facilities has established institutional expertise in the management of sensitive, confidential information including trade secrets.

**2. Security protocols to be implemented.**

The security protocols at each facility will include:

a. Both sites will create or maintain a single locked, secure work area which is subject to 24-hour video surveillance.

b. The secure work area will only be accessed by key or key card available to the experts or attorneys on the review team and designated staff under their control and supervision, with no janitorial or other access.

c. Both sites will maintain the memory card(s) in a locked safe when not in use.

d. Both sites will maintain a log of everyone who accesses the secure work area.

e. State Defendants' attorneys and designated experts will be permitted to bring their own laptops into the secure work area. Those laptops may be connected to the internet via an external wireless network while they are in the room but will not be networked in any fashion or form or connected to any of the protected equipment. Beyond material required to analyze

the memory card, no additional equipment or materials would be permitted in the secure work areas.

f. All designated experts and staff assisting them and working under their control and supervision entering the secure work area would be required to sign confidentiality agreements and be bound by the terms of the Protected Order entered in this case.

Each secure work area will include:

a. A single computer, marked "Protected," which will be air-gapped, password-protected, and not connected to any internal or external network.

b. A Direct Recording Electronic voting machine (DRE), marked Protected, that will not be used for any election or attached to any election system after being placed in the secure work area.

c. If Plaintiffs do not provide two duplicate memory cards with the malware on them for each location, a single PCMCIA duplication unit which will be used to create a single copy of the memory card. No further duplication will be allowed. If Plaintiffs provide two duplicate memory cards for each

location, then no duplication unit will be included in the work area.

d. Under no circumstances would the malware or the information on the memory card be installed on any non-Protected computer, DRE, or other unit. While attorneys and designated experts and staff working under their control and supervision would be permitted to use external hard disks and removable storage media (*e.g.*, USB drives, CD-Rs, and DVD-Rs) on their own laptops and other devices, those devices would not be permitted to be installed or connected to a Protected unit.

e. State Defendants' experts and attorneys would be authorized to install software review tools by USB drive onto the Protected devices to conduct an efficient and accurate review.

f. State Defendants would be allowed to take videos and screen shots of the workings of the software, but would only be authorized to use those screen shots if considered necessary for the provision of an expert opinion at trial. State Defendants would identify those proposed videos and screen shots to Plaintiffs and if the parties cannot agree on terms for production, they would submit the dispute to the Court.

g. Any notes taken by attorneys or their experts will be maintained in strict confidentiality in the secure work area.

**3. Individuals responsible for implementing and enforcing security protocols.**

The individuals responsible for implementing and enforcing the security protocols outlined above are:

**Theresa Payton:** Ms. Payton is the Chief Executive Officer of Fortalice Solutions. Fortalice Solutions is a full-service cybersecurity company that offers businesses and governments a full suite of cybersecurity services, including cybersecurity assessments, vendor assessments, red teaming and penetration testing, review of cybersecurity policies and procedures, and cyber incident response and analysis. She was previously the Chief Information Officer for The Office of Administration, Executive Office of the President at the White House from 2006-2008, overseeing all information technology and information security functions. She is also the co-author of numerous books and articles regarding cyber-security, including *Privacy in the Age of Big Data: Recognizing Threats*, *Defending Your Rights*, and *Protecting Your Family and Protecting Your Internet Identity: Are You Naked Online?* She has been named one of the 25 Most Influential People in Security by Security Magazine.

**Counsel for State Defendants at Taylor English:** As detailed in the attached Declaration, Taylor English has extensive experience handling highly sensitive and secure data. Its Data Security and Privacy Department regularly handles extremely sensitive information, including information regarding the operation of data centers and assisting corporations with cybersecurity breaches. The firm also regularly advises companies regarding the development of systems and best practices to protect extremely sensitive trade secrets. Individuals within the firm who can be consulted about the implementation of any security protocols include the Chair of the Data Security and Privacy Department and firm's Chief Administrative Officer, individuals with significant experience in physical facility security and protecting personal and sensitive electronic information.

**4. Names and professional backgrounds of experts who will have access to the memory card for the examination.**

The experts with access to the memory card for examination are Theresa Payton, whose background is outlined above, and Dr. Michael Shamos. Paul Brandau will assist Theresa Payton as Technical Oversight Director of State Defendants' proposed review.

Dr. Shamos has more than 50 years of experience in the field of computers generally and 39 years of experience in examining computerized

voting systems. He is the Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University in Pittsburgh, Pennsylvania. He is a member of two departments in that School, the Institute for Software Research and the Language Technologies Institute. He founded and is a Co-Director of the Institute for eCommerce at Carnegie Mellon from 1998-2004 and from 2004-2018 has been Director of the eBusiness Technology graduate program in the Carnegie Mellon University School of Computer Science. Since 2018, he has served as Director of the M.S. in Artificial Intelligence and Innovation degree program at Carnegie Mellon. Dr. Shamos received an A.B. (1968) from Princeton University in Physics; an M.A. (1970) from Vassar College in Physics; an M.S. (1972) from American University in Technology of Management, a field that covers quantitative tools used in managing organizations, such as statistics, operations research and cost-benefit analysis; an M.S. (1973), and M.Phil. (1974) and a Ph.D. from Yale University in Computer Science; and a J.D. (1981) from Duquesne University. *See* [Doc. 472-1 at ¶¶ 4-5].

Paul Brandau is the Advanced Techniques and Training Director at Fortalice Solutions. Mr. Brandau leads two Fortalice security teams in developing and implementing penetration tests and strategies for clients of Fortalice Solutions. Brandau's past experience includes time as a network

malware analyst, incident responder, and penetration tester for Booz Allen Hamilton, where he oversaw remediation actions for a high-profile cyber-intrusion into a major foreign government. Brandau also served as a Captain in the United States Air Force where he developed instruction curricula for offensive and defensive cyber tactics. Brandau holds a Bachelor of Science degree in Computer Science from Embry-Riddle Aeronautical University and a Master of Science degree from the University of San Diego.

State Defendants propose that Michael Barnes of the Secretary of State's office be able to access the secure facility when present with counsel of record or a designated expert, but he will not be allowed to touch or otherwise manipulate any of the equipment located inside the secure work area.

Each expert and counsel of record and any staff assisting in the review and working under their control and supervision will be required to sign confidentiality agreements and be bound by the terms of the Protective Order in this case prior to entering the secure work area.

**5. Transmittal of memory card contents.**

State Defendants do not propose transmitting a copy of the memory card or its contents to Dr. Shamos. The only review would take place in the two secure facilities outlined above.

**6. Receipt of memory card.**

State Defendants propose Plaintiffs make four copies of the memory card onto identical PCMCIA memory cards and deliver two copies to Fortalice Solutions and two copies to Taylor English by courier or express mail service or personal delivery to the locations. Personal delivery may be to the experts, counsel for State Defendants, or their written designees who have signed confidentiality agreements.

This 16th day of July, 2019.

Vincent R. Russo
GA Bar No. 242628
Josh Belinfante
GA Bar No. 047399
Carey A. Miller
GA Bar No. 976240
Kimberly Anderson
GA Bar No. 602807
Alexander Denton
GA Bar No. 660632
Brian E. Lake
GA Bar No. 575966
ROBBINS ROSS ALLOY
BELINFANTE LITTLEFIELD LLC
500 14th Street NW
Atlanta, GA 30318
Telephone: (678) 701-9381
Facsimile: (404) 856-3250
vrusso@robbinsfirm.com
jbelinfante@robbinsfirm.com

cmiller@robbinsfirm.com
kanderson@robbinsfirm.com
adenton@robbinsfirm.com
blake@robbinsfirm.com

*/s/Bryan P. Tyson*
Bryan P. Tyson
GA Bar No. 515411
Bryan F. Jacoutot
Georgia Bar No. 668272
TAYLOR ENGLISH DUMA LLP
1600 Parkwood Circle, Suite 200
Atlanta, GA 30339
Telephone: (678)336-7249
btyson@taylorenglish.com
bjacoutot@taylorenglish.com

*Counsel for State Defendants*

**CERTIFICATE OF COMPLIANCE**

Pursuant to L.R. 7.1(D), the undersigned hereby certifies that the foregoing STATE DEFENDANTS' NOTICE REGARDING SECURITY REVIEW OF DR. HALDERMAN'S MEMORY CARD has been prepared in Century Schoolbook 13-point, a font and type selection approved by the Court in L.R. 5.1(B).

*/s/Bryan P. Tyson*
Bryan P. Tyson
GA Bar No. 515411

**CERTIFICATE OF SERVICE**

I hereby certify that on this day, I electronically filed the foregoing STATE DEFENDANTS' NOTICE REGARDING SECURITY REVIEW OF DR. HALDERMAN'S MEMORY CARD with the Clerk of Court using the CM/ECF system, which will automatically send counsel of record e-mail notification of such filing.

This 16th day of July, 2019.

*/s/Bryan P. Tyson*
Bryan P. Tyson
GA Bar No. 515411